

Configurazione e gestione del servizio HTTP/HTTPS del certificato SSL (Secure Sockets Layer) sui punti di accesso WAP121 e WAP321

Obiettivo

Il punto di accesso può essere gestito tramite connessioni HTTP e HTTP protetto (HTTPS) quando i server HTTP/HTTPS sono configurati. Il protocollo HTTPS (Hyper Text Transfer Protocol Secure) è un protocollo di trasferimento più sicuro del protocollo HTTP. Alcuni browser Web utilizzano HTTP mentre altri utilizzano HTTPS. Un punto di accesso deve disporre di un certificato SSL valido per utilizzare il servizio HTTPS. Un certificato SSL è un certificato con firma digitale rilasciato da un'autorità di certificazione che consente al browser di comunicare con il server Web in modo protetto e crittografato.

In questo articolo viene spiegato come configurare il servizio HTTP/HTTPS sui punti di accesso WAP121 e WAP321.

Dispositivi interessati

- WAP121
- WAP321

Versione del software

- 1.0.3.4

Servizio HTTP/HTTPS

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Amministrazione > Servizio HTTP/HTTPS**. Viene visualizzata la pagina *Servizio HTTP/HTTPS*:

HTTP/HTTPS Service

Global Settings

Maximum Sessions: (Range: 1-10, Default: 5)

Session Timeout: Minute (Range: 1-60, Default: 10)

HTTP Service

HTTP Server: Enable

HTTP Port: (Range: 1025-65535, Default: 80)

Redirect HTTP to HTTPS:

HTTPS Service

HTTPS Server: Enable

HTTPS Port : (Range: 1025-65535, Default: 443)

Passaggio 2. Immettere il numero massimo di sessioni Web che includono la sessione HTTP e HTTPS da utilizzare contemporaneamente nel campo Sessioni massime. Ogni volta che un utente accede al dispositivo viene creata una sessione. Se viene raggiunta la sessione massima, l'utente successivo che tenta di accedere al dispositivo con il servizio HTTP o HTTPS viene rifiutato.

Passaggio 3. Inserire nel campo Timeout sessione il periodo di tempo massimo in minuti durante il quale un utente inattivo rimane connesso all'interfaccia Web AP.

The screenshot shows a configuration interface with three sections: Global Settings, HTTP Service, and HTTPS Service. In the Global Settings section, 'Maximum Sessions' is set to 8 and 'Session Timeout' is set to 45 minutes. In the HTTP Service section, the 'HTTP Server' checkbox is checked and labeled 'Enable', the 'HTTP Port' is set to 1025, and the 'Redirect HTTP to HTTPS' checkbox is unchecked. In the HTTPS Service section, the 'HTTPS Server' checkbox is checked and labeled 'Enable', and the 'HTTPS Port' is set to 65535. A 'Save' button is located at the bottom left of the configuration area.

Passaggio 4. Selezionare la casella di controllo **Abilita** nel campo Server HTTP per abilitare l'accesso Web tramite HTTP.

Nota: Se il server HTTP è disattivato, tutte le connessioni correnti che utilizzano HTTP verranno disconnesse.

Passaggio 5. Immettere il numero di porta da utilizzare per le connessioni HTTP nel campo Porta HTTP. Il numero di porta è compreso tra 1025 e 65535.

Passaggio 6. (Facoltativo) Per reindirizzare i tentativi di accesso HTTP di gestione sulla porta HTTP alla porta HTTPS, selezionare la casella di controllo **Reindirizza HTTP a HTTPS**. Questo campo è disponibile solo quando l'accesso HTTP è disabilitato.

Passaggio 7. Selezionare la casella di controllo **Abilita** del server HTTPS per abilitare l'accesso Web tramite HTTPS.

Nota: Se il server HTTPS è disabilitato, tutte le connessioni correnti che utilizzano HTTPS verranno disconnesse.

Passaggio 8. Immettere il numero di porta da utilizzare per le connessioni HTTPS nel campo Porta HTTPS. Il numero di porta è compreso tra 1025 e 65535.

Passaggio 9. Fare clic su **Save** per salvare le impostazioni.

Generazione di un certificato SSL

La generazione di un nuovo certificato SSL HTTP per il server Web protetto deve essere eseguita dopo che l'access point ha acquisito un indirizzo IP. Ciò garantisce che il nome comune del certificato corrisponda all'indirizzo IP dell'access point. La generazione di un nuovo certificato SSL riavvia il server Web protetto. La connessione protetta non funziona finché il nuovo certificato non viene accettato nel browser. Per generare il certificato SSL, eseguire la procedura seguente.

HTTP/HTTPS Service

Global Settings

Maximum Sessions: (Range: 1-10, Default: 5)

Session Timeout: Minute (Range: 1-60, Default: 10)

HTTP Service

HTTP Server: Enable

HTTP Port: (Range: 1025-65535, Default: 80)

Redirect HTTP to HTTPS:

HTTPS Service

HTTPS Server: Enable

HTTPS Port: (Range: 1025-65535, Default: 443)

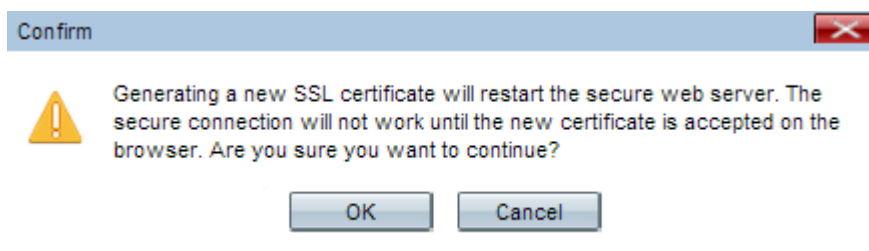
Generate SSL Certificate

SSL Certificate File Status

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 20:00:03 2019 GMT

Passaggio 1. Fare clic su **Genera** per generare un nuovo certificato SSL. Viene visualizzato il messaggio di avviso.



Passaggio 2. Fare clic su **OK** per continuare la generazione del certificato SSL.

SSL Certificate File Status

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 20:00:03 2019 GMT

Certificate Issuer Common Name: CN=192.168.1.245

Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS
 TFTP

Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS
 TFTP

File Name: No file chosen

Nell'area Stato file certificato SSL vengono visualizzate le informazioni seguenti:

- File di certificato presente - indica se il file di certificato SSL HTTP è presente o meno. Il valore predefinito è no.
- Data scadenza certificato: visualizza la data di scadenza del certificato SSL HTTP.
- Nome comune autorità di certificazione - Visualizza il nome comune dell'autorità di certificazione.

Scarica il certificato SSL

Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS
 TFTP

Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS
 TFTP

File Name: No file chosen

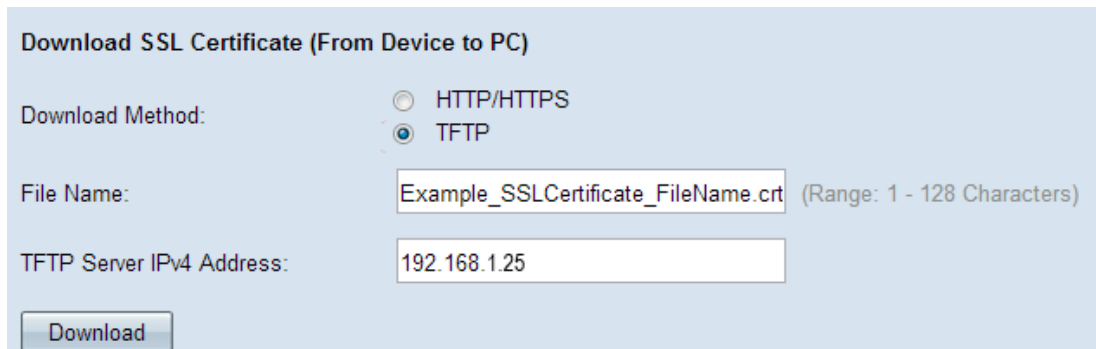
Passaggio 1. Fare clic sul file del certificato SSL appropriato dal pulsante di scelta Metodo di

download nell'area Scarica certificato SSL (da periferica a PC).

·HTTP/HTTPS: fare clic su questo pulsante di opzione se il certificato SSL deve essere scaricato da un server Web.

·TFTP: fare clic su questo pulsante di opzione se il certificato SSL deve essere scaricato da un server TFTP.

Nota: Andare al passaggio 4 se si fa clic su HTTP/HTTPS nel passaggio precedente.



Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS TFTP

File Name: (Range: 1 - 128 Characters)

TFTP Server IPv4 Address:

Passaggio 2. Se si fa clic su TFTP nel Passaggio 2, immettere il nome del file nel campo Nome file.

Passaggio 3. Immettere l'indirizzo del server TFTP nel campo Indirizzo IPv4 server TFTP.

Passaggio 4. Fare clic su **Download** per scaricare il file del certificato.

Carica il certificato SSL

Per caricare il certificato SSL, procedere come segue.



Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS TFTP

Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS TFTP

File Name: No file chosen

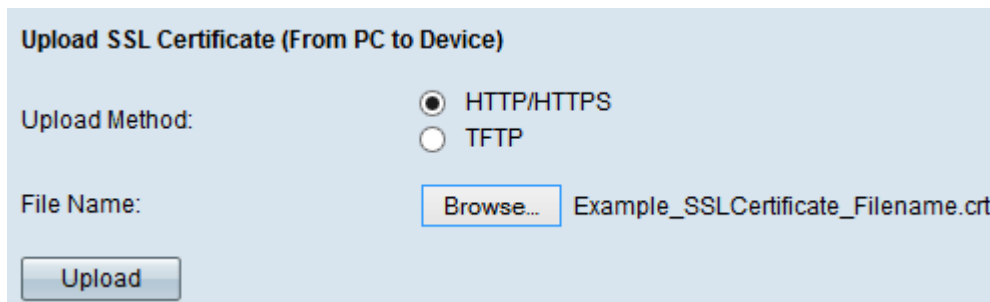
Passaggio 1. Fare clic sul pulsante di opzione appropriato nell'area Carica certificato SSL (dal PC al dispositivo).

·HTTP/HTTPS: fare clic su questo pulsante di opzione se il certificato SSL deve essere caricato con un server Web.

·TFTP: fare clic su questo pulsante di opzione se il certificato SSL deve essere caricato con un server TFTP.

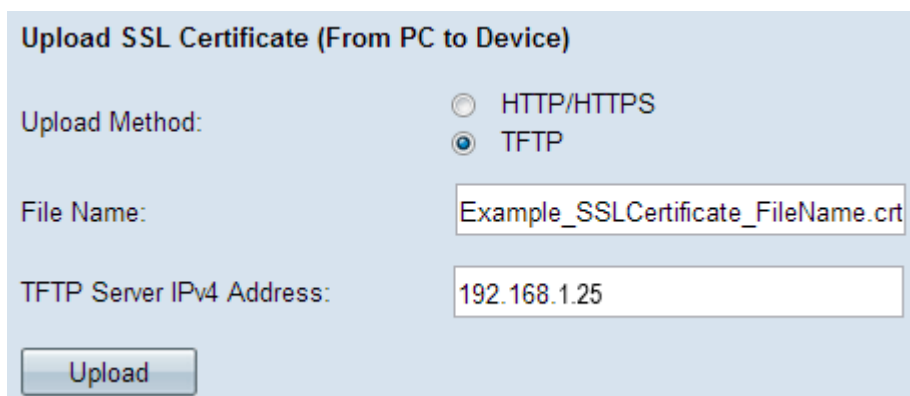
Nota: Andare al passo 4 se si fa clic su TFTP nel passo precedente.

Passaggio 2. Se si fa clic su HTTP/HTTPS, fare clic su **Scegli file** o **Sfoggia** in base al browser per cercare il file.



The screenshot shows a light blue form titled "Upload SSL Certificate (From PC to Device)". Under "Upload Method:", the "HTTP/HTTPS" radio button is selected. The "File Name:" field contains the text "Example_SSLCertificate_FileName.crt" and is preceded by a "Browse..." button. An "Upload" button is located at the bottom left of the form.

Passaggio 3. Fare clic su **Upload** per caricare il file scelto. Ignorare gli ultimi passaggi poiché si applicano solo al TFTP.



The screenshot shows the same form as above, but now the "TFTP" radio button is selected. The "File Name:" field contains "Example_SSLCertificate_FileName.crt" and the "TFTP Server IPv4 Address:" field contains "192.168.1.25". The "Upload" button remains at the bottom left.

Passaggio 4. Se si fa clic su TFTP al passaggio 2, immettere il nome del file nel campo Nome file.

Passaggio 5. Immettere l'indirizzo del server TFTP nel campo Indirizzo IPv4 server TFTP.

Passaggio 6. Fare clic su **Upload** per caricare il file del certificato.